

# COGALOIS THEORY AND DRINFELD MODULES

MARCO ANTONIO SÁNCHEZ-MIRAFUENTES, JULIO CESAR SALAS-TORRES,  
AND GABRIEL VILLA-SALVADOR

**ABSTRACT.** In this paper we generalize the results of [7] to rank one Drinfeld modules with class number one. We show that, in the present form, there does not exist a cogalois theory for Drinfeld modules of rank or class number larger than one. We also consider the torsion of the Carlitz module for the extension  $\mathbb{F}_q(T)(\Lambda_{P^n})/\mathbb{F}_q(T)(\Lambda_P)$ .

## 1. INTRODUCTION

The main goal of this paper is to obtain the analogue of the classic cogalois group. The *cogalois group* of an arbitrary field extension  $L/K$  is defined as the torsion group  $\text{tor}(L^*/K^*)$  (see [3]). The analogue for Drinfeld modules we are interested in is obtained by replacing the multiplicative structure of the field by the one given by the Drinfeld module structure. We see that when  $\rho$  is a rank one  $A$ -Drinfeld module where  $A$  is of class number one, the results of [7] can be obtained also in this case. However, we will see that there is no cogalois theory for arbitrary  $A$ -Drinfeld modules of rank one.

## 2. PRELIMINARIES AND NOTATIONS

We consider function fields  $K/\mathbb{F}_q$  where we fix a prime divisor denoted by  $\mathfrak{p}_\infty$ .  $A$  denotes the Dedekind ring consisting of the elements  $u \in K$  such that the only possible pole of  $u$  is  $\mathfrak{p}_\infty$ .

We will use the following notation along the paper.

- $k = \mathbb{F}_q(T)$  denotes the rational function field over a finite field of  $q$  elements  $\mathbb{F}_q$ .
- $R_T = \mathbb{F}_q[T]$  denotes the polynomial ring over  $T$  and such that  $k$  is the quotient field of  $R_T$ .
- $K$  is a global function field over  $\mathbb{F}_q$ .
- $C$  denotes the Carlitz module.
- $\Lambda_M = \{u \in \bar{k} \mid C_M(u) = u^M = 0\}$  with  $M \in R_T$ .
- $\mathfrak{p}_\infty$  is a fixed place of  $K$  called the *infinite prime* of  $K$ .
- $d_\infty = \deg \mathfrak{p}_\infty$  denotes the degree of  $\mathfrak{p}_\infty$ .
- $A = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ for every place } \mathfrak{p} \neq \mathfrak{p}_\infty\}$ .
- $h_K = |C_{K,0}|$  denotes the class number of  $K$ .
- $h_A = d_\infty h_K$  is the class number of the Dedekind ring  $A$ .

---

*Date:* May 9th., 2016.

*2010 Mathematics Subject Classification.* Primary 1R60; Secondary 11R18, 11R32, 11R58.

*Key words and phrases.* Drinfeld modules; cogalois theory; torsion in Drinfeld modules; cyclotomic function fields; cogalois groups.

- $\mathbb{C}_\infty = \mathbb{C}_p$  denotes the completion of an algebraic closure of the completion  $K_\infty$  of  $K$  at  $\mathfrak{p}_\infty$ .
- $\rho: A \rightarrow E\langle\tau\rangle$  is an  $A$ -Drinfeld module of generic characteristic defined over a field extension  $E$  of the field of definition  $K_\rho$  of  $\rho$ .
- $\rho[I] = \{u \in \bar{K} \mid \rho_c(u) = 0 \text{ for all } c \in I\}$  where  $I$  is an ideal of  $A$ .
- $\rho[a] = \rho[(a)]$  for  $a \in A$ .
- For a nonzero ideal  $\mathfrak{m}$  of  $A$  we let  $\Phi(\mathfrak{m}) = |(A/\mathfrak{m})^*|$ .
- $\mu_\rho(L) = \mu(L) = \{u \in L \mid \rho_a(u) = 0 \text{ for } a \in A \setminus \{0\}\}$  denotes the torsion of a Drinfeld module of an extension  $L$  of  $K$ .

For the particular case  $h_A = 1$ , necessarily we have  $d_\infty = \deg \mathfrak{p}_\infty = 1$  and  $h_K = 1$ . Therefore there exist only 5 such fields and rings  $A$  according to the classification of function fields with class number one. In this situation, we may and we will assume that  $K_\rho = K$ . We also ask whether the structural map of the Drinfeld module  $\rho, \delta: A \rightarrow E$ , is the natural embedding. The Drinfeld modules under consideration will be of rank one, unless otherwise specified. So, we have  $\deg(\rho_a) = -d_\infty v_{\mathfrak{p}_\infty}(a) = \deg a$ .

We have that  $|A/(a)| = q^{\deg a}$  is finite, and  $\deg a = \dim_{\mathbb{F}_q} A/(a)$ . If necessary, we will assume for a rank one Drinfeld module  $\rho$  that  $K_\rho = H_A$  is the Hilbert class field (see [4, §15]). Let  $H_A^+$  be the *normalizer field* for  $A$ -Drinfeld modules over  $K$ ,  $\mathfrak{p}_\infty$  for a fixed sign function  $\text{sgn}$ . We have that  $H_A^+$  is the narrow Hilbert class field with respect to  $\text{sgn}$ . We know that  $H_A^+/K$  is an abelian extension with Galois group isomorphic to  $\text{Pic}^+ A = M_A/P_A^+$  where  $M_A$  is the group of fractional ideals of  $A$  and  $P_A^+ = \{xA \mid x \in K^*, \text{sgn}(x) = 1\}$ . We have  $|\text{Pic}_A^+| = [H_A^+ : K] = \frac{q^{d_\infty}-1}{q-1} h_A$  (see [4, Theorem 14.7], [10, Theorem 13.5.30]).

If  $\rho: A \rightarrow \mathbb{C}_\infty\langle\tau\rangle$  is a rank one  $A$ -Drinfeld module, then  $\rho = \rho^\Gamma$  where  $\Gamma = A\bar{\pi}$  is a lattice with  $\bar{\pi} \in \mathbb{C}_\infty \setminus \{0\}$  and the exponential function associated to  $\rho$  is given by  $\text{ex}_\Gamma(x) = x \prod_{\gamma \in \Gamma \setminus \{0\}} (1 - \frac{x}{\gamma})$ . Thus  $\text{ex}_\Gamma(\gamma) = 0$  if and only if  $\gamma \in \Gamma$ . We define  $\lambda_a := \text{ex}_\Gamma(\frac{\bar{\pi}}{a})$  for  $a \in A \setminus \{0\}$ . From the functional equation  $\text{ex}_\Gamma(au) = \rho_a(\text{ex}_\Gamma(u))$  we obtain that  $\rho_a(\lambda_a) = 0$ . Further  $\rho_m(\lambda_{mn}) = \lambda_n$  for  $n, m \in A$ .

**Remark 2.1.** We have that  $\lambda_a$  is a generator of the  $A$ -module  $\rho[a]$ .

### 3. GENERAL RESULTS ON DRINFELD MODULES

The following results will be used along the paper.

**Proposition 3.1.** *Let  $\rho$  be an  $A$ -Drinfeld module of rank one and let  $a \in A$  be nonzero. Then  $K(\rho[a])/K$  is an abelian extension and  $\text{Gal}(K(\rho[a])/K)$  is isomorphic to a subgroup of the group  $(A/(a))^*$ .  $\square$*

**Proposition 3.2.** *Let  $\mathfrak{P}$  be a nonzero prime ideal of  $A$ . Let  $m \in \mathbb{N}$  and  $K(\mathfrak{P}^m) := H_A^+(\rho[\mathfrak{P}^m])$ . Then the extension  $K(\mathfrak{P}^m) = H_A^+(\rho[\mathfrak{P}^m])/H_A^+$  is totally ramified in  $\mathfrak{F}$ , where  $\mathfrak{F}$  is the prime divisor of  $H_A^+$  above  $\mathfrak{P}$  and the ramification index is equal to  $\Phi(\mathfrak{P}^m)$ . Furthermore, the extension  $K(\mathfrak{P}^m)/H_A^+$  is unramified at every prime divisor other than  $\mathfrak{P}$  and the primes above  $\mathfrak{p}_\infty$ . We also have  $[K(\mathfrak{P}^m) : H_A^+] = \Phi(\mathfrak{P}^m)$ .*

*Finally,  $\mathfrak{p}_\infty$  decomposes fully in  $H_A/K$  and is totally ramified in  $H_A^+/H_A$ .*

*Proof.* See [4, Proposition 14.4, Theorem 15.6], [10, Proposition 13.5.41, Theorem 13.5.35].  $\square$

**Corollary 3.3.** *For any nonzero ideal  $\mathfrak{m}$  of  $A$ ,  $K(\mathfrak{m}) := H_A^+(\rho[\mathfrak{m}])/H_A^+$  is a Galois extension with Galois group isomorphic to  $(A/\mathfrak{m})^*$ . The ramified finite primes are precisely the prime ideals  $\mathfrak{P}$  dividing  $\mathfrak{m}$  with ramification index equal to  $\Phi(\mathfrak{P}^e)$  where  $\mathfrak{P}^e$  is the exact power of  $\mathfrak{P}$  that divides  $\mathfrak{m}$ .*

*Proof.* [4, §16], [10, Corollary 13.5.42].  $\square$

**Theorem 3.4.** *If  $A$  is arbitrary and  $\rho$  is any  $A$ -Drinfeld module, then  $\mu_\rho(L)$  is a finite set for any finite extension  $L$  of  $K$ .*

*Proof.* [1, 2, 6, 9].  $\square$

**Remark 3.5.** The first proof of Theorem 3.4 was given by Denis in [1, Théorème 1], where he proves that the number of elements with height bounded by a fixed real number  $D$ , is finite and that the torsion elements are precisely the elements of height 0. To show only that the torsion is finite, the proof can be reduced to the case  $A = R_T$  ([6, Proposition 1], [2, Remark 2.8]) as follows: if  $\rho: A \rightarrow E\langle\tau\rangle$  is an  $A$ -Drinfeld module over  $E$ , we choose  $T \in K$  such that the pole divisor of  $T$  is  $\mathfrak{p}_\infty^n$  for some  $n \geq 1$ . Then  $A$  is the integral closure of  $R_T$  in  $K$  and  $\rho' = \rho \circ i: R_T \rightarrow E\langle\tau\rangle$  is an  $R_T$ -Drinfeld module over  $E$  where  $i$  is the natural embedding. Then  $\mu_{\rho'}(L) = \mu_\rho(L)$ , being the fact  $\mu_{\rho'}(L) \subseteq \mu_\rho(L)$  clear. Now, if  $x \in \mu_\rho(L)$ , then  $\rho_a(x) = 0$  with  $a \in A \setminus \{0\}$ . Consider  $\alpha_0, \dots, \alpha_{n-1} \in R_T$ ,  $\alpha_0 \neq 0$  and  $\alpha_0 + \alpha_1 a + \dots + \alpha_{n-1} a^{n-1} + a^n = 0$ , so  $\rho_{\alpha_0}(x) = 0$  and thus  $x \in \mu_{\rho'}(L)$ .

Once we have reduced to the case  $R_T$ , the proof of the finiteness of  $\mu_\rho(L)$  can be obtained over a finite extension  $L$  of  $K_{\mathfrak{p}}$ , where  $K_{\mathfrak{p}}$  is the completion of  $K$  at  $\mathfrak{p} \neq \mathfrak{p}_\infty$  proving that if  $x \in \mu_\rho(L)$ , then  $v_{\mathfrak{p}}(x) \geq c$  for some  $c$  and therefore  $\overline{\mu_\rho(L)}$  is a compact discrete set, hence finite ([6, Proposition 1]).

In the particular case of rank one over  $R_T$  and  $A$  with  $h_A = 1$ , we have  $\mu_\rho(L) = \rho[a]$  for some  $a \in A \setminus \{0\}$ . In particular,  $\mu_C(L) = \Lambda_M$  for some  $M \in R_T \setminus \{0\}$  in the Carlitz module case. This is a very particular case of the general case of Drinfeld modules of rank one.

**Proposition 3.6.** *Let  $L/E$  be a finite extension and let  $\rho$  be a Drinfeld module of rank one. Then there exists an ideal  $\mathfrak{b}$  of  $A$  such that  $\mu_\rho(L) = \rho[\mathfrak{b}]$ . In particular, if  $\rho = C$  is the Carlitz module,  $\mu_C(L) = \Lambda_M$  for some  $M \in R_T$ .*

*Proof.* Let  $x \in \mu_\rho(L)$  and choose  $a \in A$ ,  $a \neq 0$  such that  $\rho_a(x) = 0$ . Consider the annihilator of  $x$ :  $\text{an}(x) := \{b \in A \mid \rho_b(x) = 0\} = \mathfrak{a}$ . Then  $\mathfrak{a}$  is a nonzero ideal of  $A$ . Let  $M := A \cdot x = \{\rho_b(x) \mid b \in A\}$ . We have that  $M \subseteq L$  since  $L$  is an  $A$ -module and  $M \cong A/\mathfrak{a}$ . On the other hand  $\rho[\mathfrak{a}] \cong A/\mathfrak{a}$  because  $\rho$  is of rank one. Clearly we have that  $M \subseteq \rho[\mathfrak{a}]$  and since both sets are of the same cardinality  $|A/\mathfrak{a}|$ , it follows that  $M = \rho[\mathfrak{a}]$ . Therefore  $\rho[\mathfrak{a}] \subseteq \mu_\rho(L)$ .

Since  $\mu_\rho(L)$  is finite, we write  $\mu_\rho(L) = \{x_1, \dots, x_m\}$  and let  $\mathfrak{a}_i := \text{an}(x_i)$ ,  $1 \leq i \leq m$ . Let  $\mathfrak{b} = \text{lcm}\{\mathfrak{a}_i \mid 1 \leq i \leq m\} = \cap_{i=1}^m \mathfrak{a}_i$ . Let  $\mathfrak{c}_i$  be an integral ideal such that  $\mathfrak{b} = \mathfrak{a}_i \mathfrak{c}_i$ ,  $1 \leq i \leq m$ . We have  $\rho_b(x_i) = 0$  for all  $b \in \mathfrak{b}$  and for all  $1 \leq i \leq m$ . It follows that  $\mu_\rho(L) \subseteq \rho[\mathfrak{b}]$ .

Let now  $x \in \rho[\mathfrak{b}]$ . We claim that  $\{\mathfrak{c}_i\}_{i=1}^m$  are relatively primes, that is,  $A = \sum_{i=1}^m \mathfrak{c}_i = \text{lcm}\{\mathfrak{c}_i \mid 1 \leq i \leq m\}$ . Otherwise, we would have a nonzero prime ideal  $\mathfrak{p}$  dividing  $\mathfrak{c}_i$  for all  $1 \leq i \leq m$ . Let  $\mathfrak{d}_i$  be such that  $\mathfrak{c}_i = \mathfrak{d}_i \mathfrak{p}$ , hence  $\mathfrak{b} = \mathfrak{a}_i \mathfrak{c}_i = \mathfrak{a}_i \mathfrak{d}_i \mathfrak{p}$  and therefore  $\mathfrak{b} \mathfrak{p}^{-1} = \mathfrak{a}_i \mathfrak{d}_i$  so it follows that  $\mathfrak{a}_i$  divides  $\mathfrak{b} \mathfrak{p}^{-1}$  for all  $i$  from it would follow  $\mathfrak{b} \mid \mathfrak{b} \mathfrak{p}^{-1}$  which is absurd. This shows that  $\text{lcm}\{\mathfrak{c}_i \mid 1 \leq i \leq m\} = A$ .

Let  $c_i \in \mathfrak{c}_i$ ,  $1 \leq i \leq m$ , be such that  $1 = \sum_{i=1}^m c_i$ . For all  $1 \leq i \leq m$  and for all  $d \in \mathfrak{a}_i$ , we have  $dc_i \in \mathfrak{a}_i \mathfrak{c}_i = \mathfrak{b}$  so that

$$\rho_{dc_i}(x) = \rho_d(\rho_{c_i}(x)) = \rho_{c_i}(\rho_d(x)) = 0,$$

which implies  $\rho_{c_i}(x) \in \rho[\mathfrak{a}_i] \subseteq \mu_\rho(L)$ . Therefore

$$x = \rho_1(x) = \sum_{i=1}^m \rho_{c_i}(x) \in \mu_\rho(L),$$

thus we obtain  $\rho[\mathfrak{b}] \subseteq \mu_\rho(L)$  and hence  $\rho[\mathfrak{b}] = \mu_\rho(L)$ .  $\square$

**Proposition 3.7.** *Let  $\rho$  be an  $A$ -Drinfeld module of rank one over  $E \subseteq H_A^+$ . Let  $q > 2$  and  $\mathfrak{m}$  a nonzero ideal of  $A$ . Consider the extension  $K(\mathfrak{m}) = H_A^+(\rho[\mathfrak{m}])/H_A^+$ . Then  $\mu_\rho(K(\mathfrak{m})) = \rho[\mathfrak{m}]$ .*

*Proof.* It suffices to show that  $\mu_\rho(K(\mathfrak{m})) \subseteq \rho[\mathfrak{m}]$ . If  $u \in \mu_\rho(K(\mathfrak{m}))$ , then  $\rho_a(u) = 0$  for some  $a \in A \setminus \{0\}$ . Let  $\text{an}_\rho(u) = \mathfrak{c} \neq 0$ . From Proposition 3.6 it follows that  $\rho[\mathfrak{c}] \subseteq K(\mathfrak{m})$ ,  $K(\rho[\mathfrak{c}]) \subseteq K(\rho[\mathfrak{m}])$  and  $K(\mathfrak{c}) \subseteq K(\mathfrak{m})$ . From Proposition 3.2 it follows, analyzing the ramification index of each prime in the extensions  $K(\mathfrak{c})/H_A^+$  and  $K(\mathfrak{m})/H_A^+$ , that  $\mathfrak{c} \mid \mathfrak{m}$  and therefore  $u \in \rho[\mathfrak{c}] \subseteq \rho[\mathfrak{m}]$ .  $\square$

#### 4. RADICAL EXTENSIONS

Let  $K/\mathbb{F}_q$  be a function field and let  $\mathfrak{p}_\infty$  be a fixed prime divisor. Let us consider  $\delta : A \rightarrow E$  the natural embedding and  $\rho : A \rightarrow E\langle\tau\rangle$  a rank one Drinfeld module. As before, we consider function field extensions  $L/K$  such that  $E \subseteq K \subseteq L \subseteq \bar{k}$ . Since this type of extensions are  $E$ -algebras, we may give them an  $A$ -module structure using the map  $\rho$ . The first object to consider, associated to the extension  $L/K$ , is the following:

$$\text{DrinT}(L/K) = \{u \in L \mid \text{there exists } m \in A \setminus \{0\} \text{ such that } \rho_m(u) \in K\}.$$

Note that  $\text{DrinT}(L/K) \subseteq L$  is a subgroup of the additive group  $L$ . On the other hand,  $\text{DrinT}(L/K)$  is an  $A$ -module and the  $A$ -module  $\text{DrinT}(L/K)/K$  is of  $A$ -torsion. The module  $\text{Drincog}(L/K) = \text{DrinT}(L/K)/K$  will be called the *Drinfeld cogalois module* of the extension  $L/K$ . We have that  $\text{Drincog}(L/K)$  is analogous to the group  $T(L/K)/K^*$  in a field extension  $L/K$  where  $T(L/K)$  denotes the usual torsion group associated to the extension  $T(L/K)$ , that is,  $T(L/K) = \{u \in L \mid \text{there exists } n \in \mathbb{N} \text{ such that } u^n \in K\}$  (see [3]).

**Definition 4.1.** We say that an extension  $L/K$  is *radical* if there exists a set  $X \subseteq \text{DrinT}(L/K)$  such that  $L = K(X)$ . We will say that  $L/K$  is *pure* if for any irreducible  $m \in A$  and for each  $\lambda_m \in L$ , we have  $\lambda_m \in K$ . Finally we will say that  $L/K$  is a *cyclotomic coradical extension* if it is radical, separable and pure.

**4.1. Reduction to the case  $R_T$ .** In this subsection we show how we may reduce the general case to the case  $A = R_T$ .

Let  $A$  and  $K$  be arbitrary. Let  $T \in A$  be such that  $\mathfrak{N}_T = \mathfrak{p}_\infty^n$ , for some  $n \geq 1$ . Consider  $R_T = \mathbb{F}_q[T]$  and  $k = \mathbb{F}_q(T)$ . Let  $\rho : A \rightarrow E\langle\tau\rangle$  be a  $A$ -Drinfeld module of rank  $r_\rho$ . Let  $\iota : R_T \rightarrow A$  be the natural embedding and let  $\rho' : R_T \rightarrow E\langle\tau\rangle$  be given by  $\rho' = \rho \circ \iota$ . Let  $r_{\rho'}$  be the rank of  $\rho'$ . Then

**Proposition 4.2.**  $r_{\rho'} = d_\infty n r_\rho$ .

*Proof.* We have  $\deg_{R_T} \alpha_0 = -v_{\mathcal{P}_\infty}(\alpha_0)$ , where  $\mathcal{P}_\infty$  is the pole of  $T$ . Further, we have  $d_{\mathcal{P}_\infty} = 1$  and

$$\deg_A \alpha_0 = -d_\infty v_{\mathfrak{p}_\infty}(\alpha_0) = -d_\infty e(\mathfrak{p}_\infty | \mathcal{P}_\infty) v_{\mathcal{P}_\infty}(\alpha_0) = d_\infty n \deg_{R_T} \alpha_0.$$

It follows that

$$\begin{aligned} \deg \rho_{\alpha_0} &= r_{\rho'} \deg_{R_T} \alpha_0 \quad \text{and} \\ \deg \rho_{\alpha_0} &= r_\rho \deg_A \alpha_0 = d_\infty n \deg_{R_T} \alpha_0. \end{aligned}$$

Therefore  $r_{\rho'} = d_\infty n r_\rho$ .  $\square$

**Proposition 4.3.** *Let  $L/E$  be a finite extension. Then with the conditions of Proposition 4.2, we have  $\text{Drincog}_\rho(L/E) = \text{Drincog}_{\rho'}(L/E)$ .*

*Proof.* Let  $x \in \text{Drincog}_{\rho'}(L/E)$ . There exists  $\alpha_0 \in R_T$ ,  $\alpha_0 \neq 0$ , such that  $\rho'_{\alpha_0}(x) \in E$ . Therefore  $\rho'_{\alpha_0}(x) = \rho_{\iota\alpha_0}(x) = \rho(\iota\alpha_0)(x) = \rho(\alpha_0)(x) = \rho_{\alpha_0}(x) \in E$ . It follows that  $x \in \text{Drincog}_\rho(L/E)$ , and therefore  $\text{Drincog}_{\rho'}(L/E) \subseteq \text{Drincog}_\rho(L/E)$ .

Now let  $x \in \text{Drincog}_\rho(L/E)$ . There exists  $a \in A$ ,  $a \neq 0$  such that  $\rho_a(x) \in E$ . Since  $A$  is the integral closure of  $R_T$  in  $K$ , there exist  $\alpha_0 \neq 0, \alpha_1, \dots, \alpha_{m-1} \in R_T$  such that  $\alpha_0 + \alpha_1 a + \dots + \alpha_{m-1} a^{m-1} + a^m = 0$ . Therefore, considering  $\alpha_m = 1$ , we obtain

$$0 = \rho_0(x) = \rho_{\sum_{i=0}^m \alpha_i a^i}(x) = \sum_{i=0}^m \rho_{\alpha_i} \rho_{a^i}(x) = \rho_{\alpha_0}(x) + \sum_{i=1}^m \rho_{\alpha_i}(\rho_a \circ \dots \circ \rho_a)(x) \in E$$

which implies  $\rho_{\alpha_0}(x) \in E$ . Hence  $x \in \text{Drincog}_{\rho'}(L/E)$ . This finishes the proof.  $\square$

Now we return to the general case.

In the following examples, we consider the field  $\mathbb{F}_q$  with  $q > 2$ .

**Example 4.4.** Let  $A = R_T$  and  $E = k$ . The extension  $k(\rho[m])/k$ , with  $m \in A$  non constant, is radical since there exists  $W = \rho[m] \subseteq \text{DrinT}(k(\rho[m])/k)$  such that  $k(\rho[m]) = k(W)$ . It is also a separable extension but it is not pure since from Proposition 3.7, we have that  $\mu(k(\rho[m]))$  is equal to  $\rho[m]$  and if  $c$  is an irreducible factor of  $m$ ,  $\lambda_c \in \rho[m]$  does not belong to  $k$ . Therefore  $k(\rho[m])/k$  is not a cyclotomic coradical extension.

**Example 4.5.** Let  $A = R_T$  and  $E = k$ . Let  $c \in A$  be an irreducible polynomial. The extension  $k(\rho[c^n])/k(\rho[c])$  is cyclotomic coradical since it is clear that is radical and separable because the polynomial with coefficients in  $k$ ,  $\rho_{c^n}(U)$ , is separable. On the other hand, let  $d \in A$  be an irreducible polynomial in such a way that  $\lambda_d \in k(\rho[c^n])$ . From Proposition 3.7, we have that  $d \mid c^n$  and thus  $d \mid c$ . It follows that the extension is pure.

The same argument may be applied for arbitrary  $A$ ,  $\rho$  of rank one,  $\mathfrak{c}$  a nonzero ideal of  $A$  and the extension  $K(\mathfrak{c}^n)/K(\mathfrak{c})$  for  $n \in \mathbb{N}$ .

Let us assume that  $L/K$  is a radical extension. Therefore there exist  $\alpha_i \in L$  and  $a_i \in A$  such that  $\rho_{a_i}(\alpha_i) = \beta_i \in K$  and  $L = K(\{\alpha_i\})$ . Now we take  $\alpha_i$  arbitrary. We denote such element only by  $\alpha$ . We define

$$\varphi_{\overline{\alpha}} : A \rightarrow \text{Drincog}(L/K)$$

for  $\varphi_{\overline{\alpha}}(a) = \overline{\rho_a(\alpha)}$ .

This map is well defined and  $I = \ker(\varphi_{\overline{\alpha}})$  is a nonzero ideal of  $A$  distinct from  $A$  itself. Hence, in case  $h_A = 1$ , there exists  $a \in A$  such that  $I = (a)$ . We say that  $\alpha$

is of order  $a$ . This definition is ambiguous since other generator of  $I$  might be used as the order. However we will accept this ambiguity.

**Theorem 4.6.** *Let  $h_A = 1$  and  $E = K$ . Let  $L/K$  be a radical extension, say  $L = K(\{\alpha_i\})$ . Then  $L/K$  is a Galois extension if and only for each  $\alpha_i$  of order  $a_i$ , we have  $\lambda_{a_i} \in L$ .*

*Proof.* We first consider the case  $L/K$  is a Galois extension. Let  $\alpha = \alpha_i$  be of order  $a = a_i$ . Consider the polynomial  $f(U) = \rho_a(U) - \beta \in K[U]$ , where  $\beta = \rho_a(\alpha)$ . Now  $f(U) = \prod (U - (\alpha + \rho_b(\lambda_a)))$ , so that  $\text{Irr}(U, \alpha, K)$  divides  $f(U)$ . It follows that the conjugates of  $\alpha$  in  $L$  are of type

$$\{\alpha + \xi_1, \dots, \alpha + \xi_s\},$$

with  $\xi_j \in \rho[a]$ . Note that this set is contained in  $L$ .

Let  $\xi_i = \rho_{b_i}(\lambda_a)$  for some  $b_i \in A$  and let  $B$  be the  $A$ -module generated by  $\{\xi_1, \dots, \xi_s\} \subseteq \rho[a]$ . There exists  $a' \in A$  such that  $a' \mid a$  and  $B = \rho[a']$ . Let  $\beta' = \rho_{a'}(\alpha)$ . Consider the polynomial  $g(U) = \rho_{a'}(U) - \beta' \in K[U]$ . We have  $\text{Irr}(U, \alpha, K) \mid g(U)$  and  $g(\alpha) = 0$ . Therefore  $a' \in I = \ker(\varphi_{\bar{\alpha}})$ . Hence  $a \mid a'$  and it follows that  $a' = au$  with  $u \in A$  a unit. So,  $\lambda_a \in L$ .

Conversely, let  $a$  be the order of  $\bar{\alpha}$ . Every conjugate of  $\alpha$  is of the form  $\alpha + \rho_b(\lambda_a) \in L$ . Thus  $L/K$  is a normal extension. Since  $\alpha$  is separable over  $K$ , it follows that the extension  $L/K$  is a Galois extension.  $\square$

**Proposition 4.7.** *Let  $L/E$  be an extension such that  $L = K(\alpha, \beta)$  and such that there exist  $m, n \in A$  with  $\rho_m(\alpha) \in K$  and  $\rho_n(\beta) \in K$  being  $m$  and  $n$  relatively prime, that is,  $(m) + (n) = A$ . Then  $L = K(\alpha + \beta)$ , that is,  $\alpha + \beta$  is a primitive element for the extension and it also belongs to  $\text{DrinT}(L/K)$ .*

*Proof.* We have  $K(\alpha + \beta) \subseteq K(\alpha, \beta)$ . Let  $\xi_1 = \rho_m(\alpha)$  and  $\xi_2 = \rho_n(\beta)$ . Then  $\rho_m(\alpha + \beta) = \rho_m(\alpha) + \rho_m(\beta) = \xi_1 + \rho_m(\beta) \in K(\alpha + \beta)$  and  $\rho_n(\alpha + \beta) = \rho_n(\alpha) + \rho_n(\beta) = \rho_n(\alpha) + \xi_2 \in K(\alpha + \beta)$ . Thus  $\rho_m(\beta), \rho_n(\alpha) \in K(\alpha + \beta)$ .

Let  $s_1, s_2 \in A$  be such that  $1 = ms_1 + ns_2$ . Then

$$\alpha = \rho_1(\alpha) = \rho_{ms_1+ns_2}(\alpha) = \rho_{s_1}(\xi_1) + \rho_{s_2}(\rho_n(\alpha)) \in K(\alpha + \beta)$$

and

$$\beta = \rho_1(\beta) = \rho_{ms_1+ns_2}(\beta) = \rho_{s_1}(\rho_n(\beta)) + \rho_{s_2}(b) \in K(\alpha + \beta),$$

so that  $K(\alpha, \beta) = K(\alpha + \beta)$ . Furthermore

$$\rho_{mn}(\alpha + \beta) = \rho_n(\rho_m(\alpha)) + \rho_m(\rho_n(\beta)) \in K.$$

$\square$

We observe that the result can be generalized to extensions  $L/E$  such that  $L = E(\alpha_1, \dots, \alpha_s)$  and such that there exist  $m_i \in A$  with  $\rho_{m_i}(\alpha_i) = \beta_i \in E$  and the elements  $m_i$  are pairwise relatively prime.

Next we will give some definitions which are analogous to the ones given in [8]. Here, we consider  $A$  of class number one and  $E = K$ . As before, let  $\rho$  denote a Drinfeld module. Let  $a \in A \setminus \{0\}$ ,  $K$  be any finite extension of  $k(\rho[a])$  and  $z \in K \setminus K_a$ , where  $K_a = \{\rho_a(y) \mid y \in K\}$ . Consider the polynomial  $G(U) = \rho_a(U) - z$ . The decomposition field of  $G(U)$  will be called a *Drinfeld-Kummer extension*. Multiplying  $a$  by a suitable constant, we may assume that  $G(U)$

is a monic polynomial. This type of extensions will be denoted by  $K_{a,z}$ . On the other hand, note that in general the polynomial  $G(U)$  is not irreducible over  $K$ . Let  $G_1(U), \dots, G_s(U)$  be the irreducible monic factors of  $G(U)$ .

Next proposition establishes some properties of these extensions.

**Proposition 4.8.** *Let  $K$  be a finite extension of  $k(\rho[a])$ . Let  $z \in K \setminus K_a$  and let  $K_{a,z}$  be the associated Drinfeld–Kummer extension. Then*

- (1)  $G(U)$  is a separable polynomial of degree  $q^m$  with  $m = \deg a$ .
- (2) If  $\alpha \in \bar{k}$  is any root of  $G(U)$ , then  $W = \{\alpha + \lambda \mid \lambda \in \rho[a]\}$  is the set of all roots of  $G(U)$  and  $K_{a,z} = K(\alpha)$ .
- (3) There exists  $s \in \mathbb{N}$  such that  $[K_{a,z} : K] = p^s$ .

*Proof.* (1) By the conditions satisfied by  $\rho$ , it is clear that  $G(U)$  is separable and of the claimed degree.

(2) Since  $\rho$  is a linear map it follows that  $W$  is the set of all roots of  $G(U)$ .

(3) Consider the Galois group  $\text{Gal}(L/K)$  of the extension  $L/K$ . Consider  $\sigma \in \text{Gal}(L/K)$ . Then  $\sigma(\alpha) = \alpha + \lambda_\sigma$  with  $\lambda_\sigma \in \rho[a]$ . We define  $\Theta : \text{Gal}(L/K) \rightarrow \rho[a]$  given by  $\Theta(\sigma) = \lambda_\sigma$ . We have that  $\Theta$  is well defined and since  $\sigma(\tau(\alpha)) = \sigma(\alpha + \lambda_\tau) = \alpha + \lambda_\sigma + \lambda_\tau$ , it follows that  $\Theta$  is a group homomorphism. Finally, if  $\Theta(\sigma) = 0$ , then  $\lambda_\sigma = 0$ , that is, it follows from the definition of  $\Theta$ , that the automorphism  $\sigma$  is the identity map. Therefore  $\Theta$  is a group monomorphism. In particular  $\text{Gal}(L/K)$  is an elementary  $p$ -abelian group, that is, for each  $\sigma \in \text{Gal}(L/K)$  we have  $p\sigma = 1$ . The result follows.  $\square$

## 5. CYCLOTOMIC CORADICAL EXTENSIONS

Cyclotomic coradical extensions have several properties analogous to the ones of classical cogalois extensions.

**Lemma 5.1.** *Let  $E \subseteq L \subseteq L'$  be a tower of fields. Then  $L'/E$  is pure if and only if  $L'/L$  and  $L/E$  are pure.*

*Proof.* Analogous to [7, Lemma 5.1].  $\square$

**Proposition 5.2.** *Let  $E \subseteq L \subseteq L'$  be a tower of fields. Then*

- (1) *There is an exact sequence of  $A$ -modules*  

$$0 \rightarrow \text{Drincog}(L/E) \rightarrow \text{Drincog}(L'/E) \rightarrow \text{Drincog}(L'/L).$$
- (2) *If the extension  $L'/E$  is cyclotomic coradical, then the extension  $L'/L$  is cyclotomic coradical.*
- (3) *If the extension  $L'/E$  is radical and the extensions  $L'/L$  and  $L/E$  are cyclotomic coradical, then  $L'/E$  is cyclotomic coradical.*

*Proof.* Similar to [7, Proposition 5.2].  $\square$

Note that if  $L/E$  is a Galois field extension, then  $\mu_\rho(L)$  is a  $G = \text{Gal}(L/E)$ -module with the natural action.

Next theorem holds for any finite extension and any  $A$ -Drinfeld module  $\rho$ .

**Theorem 5.3.** *Let  $L/E$  be a finite Galois extension and let  $G$  be its Galois group. Then the map  $\phi : \text{Drincog}(L/E) \rightarrow Z^1(G, \mu(L))$  given by  $\phi(u + E) = f_u$  where  $f_u(\sigma) = \sigma(u) - u$ , is a group isomorphism.*

*Proof.* Analogous to [7, Theorem 5.4].  $\square$

**Corollary 5.4.** *Let  $L/E$  be a finite extension. Then the  $A$ -module  $\text{Drincog}(L/E)$  is finite.*

*Proof.* We take the Galois closure  $\tilde{L}/E$  of  $L/E$ . The result follows from Proposition 5.2, Theorem 5.3 and from Theorem 3.4.  $\square$

Several results from [7] also hold in our situation.

From now on, the following results only hold for  $A$  such that  $h_A = 1$ .

**Proposition 5.5.** *Let  $A$  be such that  $h_A = 1$  and  $L/E$  be a field extension such that*

$$[L : E] = \ell$$

*with  $\ell$  a prime number different from  $p = \text{char } k$ . Then  $L/E$  is not a cyclotomic coradical extension.*

*Proof.* Analogous to [7, Proposition 6.1].  $\square$

**Corollary 5.6.** *Let  $A$  with  $h_A = 1$  and let  $L/E$  be a Galois extension such that*

$$[L : E] = p^s n$$

*with  $p \nmid n$  and  $n > 1$ . Then  $L/E$  is not a cyclotomic coradical extension.*

*Proof.* Analogous to [7, Corollary 6.2].  $\square$

**Corollary 5.7.** *If  $h_A = 1$  and  $L/E$  is a cyclotomic coradical Galois extension, then  $[L : E]$  is of the form  $p^s$ , with  $s \in \mathbb{N}$ .*  $\square$

**Lemma 5.8.** *If  $h_A = 1$  and if  $L/E$  is an extension such that  $[L : E] = p^s$  with  $s \in \mathbb{N}$ , then  $L/E$  is pure.*

*Proof.* Analogous to [7, Lemma 6.4].  $\square$

As a consequence of the previous results, we obtain

**Theorem 5.9.** *Assume  $h_A = 1$ . A Galois extension  $L/E$  is cyclotomic coradical if and only if it is radical, separable and  $[L : E] = p^s$  for some  $s \in \mathbb{N}$ .*  $\square$

**Theorem 5.10.** *Assume  $h_A = 1$  and let  $L/E$  be a pure extension. Assume that  $L = E(\alpha)$  and that there exists an irreducible element  $d \in A$  such that  $\rho_d(\alpha) = x \in E$ . Then  $L/E$  is a cyclotomic coradical extension and there exists  $s \in \mathbb{N}$  such that  $[L : E] = p^s$ .*

*Proof.* Similar to [7, Theorem 6.7].  $\square$

As a consequence we obtain:

**Theorem 5.11.** *If  $L/E$  is a cyclotomic coradical extension and if  $h_A = 1$ , then  $[L : E] = p^n$  for some  $n \geq 0$ .*

*Proof.* Let  $L/E$  be a cyclotomic coradical extension. Then  $L = E(\alpha_1, \dots, \alpha_t)$ , so that  $\rho_{m_i}(\alpha_i) = a_i \in E$  where  $m_i \in A$ . Taking  $m_i = d_1^{\varepsilon_{1,i}} \cdots d_{r_i}^{\varepsilon_{r_i,i}}$ ,  $\delta_{i,j} = \rho_{\frac{m_i}{d_{i,j}}}(\alpha_i)$  we have that  $\rho_{d_{i,j}}(\delta_{i,j}) = a_i$ . It follows that there exists a field tower

$$E \subseteq E(\beta_1) \subseteq E(\beta_1, \beta_2) \subseteq \cdots \subseteq E(\beta_1, \dots, \beta_s) = L$$

where for each  $i = 1, \dots, s$  we have that  $\rho_{d_i}(\beta_i) = b_i \in E(\beta_1, \dots, \beta_{i-1})$  and

$$(1) \quad [L : E] = \prod_{i=1}^s [E(\beta_1, \dots, \beta_i) : E(\beta_1, \dots, \beta_{i-1})].$$



From equation (1) follows that it suffices to show that if  $L = E(\alpha)$  with  $\rho_m(\alpha) = a \in E$  and if  $m \in A$  is irreducible, and so  $L/E$  is a cyclotomic coradical extension, then  $[L : E] = p^i$  for some  $i \in \mathbb{N}$ . The later claim follows from Lemma 5.10.  $\square$

**Corollary 5.12.** *With the notations of Theorem 5.11 we have*

$$E(\alpha) \cap E(\lambda_d) = E, \quad [L : E] = [L(\lambda_d) : E(\lambda_d)]$$

and

$$\text{Irr}(u, \alpha, E) = \text{Irr}(u, \alpha, E(\lambda_d)) = F_1(u) = \prod (u - (\alpha + \lambda_d^A)).$$

*Proof.* It follows from the proof of Theorem 5.11.  $\square$

Next corollary is analogous to Theorem 5.9 except that we do not assume that the extension  $L/E$  is Galois.

**Corollary 5.13.** *Assume  $h_A = 1$ . An extension  $L/E$  is cyclotomic coradical if and only if it is separable, radical and  $[L : E] = p^m$  for some  $m \in \mathbb{N}$ .*

*Proof.* It follows from Theorem 5.11 and Lemma 5.8.  $\square$

## 6. SOME COMPUTATIONS

Let  $L/E$  be a finite cyclotomic coradical Galois extension. Therefore we have that  $L = E(\alpha_1, \dots, \alpha_s)$  for some  $\alpha_i \in L$  and for each  $\alpha_i$  there exists  $a_i \in A$  such that  $\beta_i = \rho_{a_i}(\alpha_i) \in E$ . We may consider the polynomials  $f_i(U) = \rho_{a_i}(U) - \beta_i$ . The set of roots of each polynomial  $f_i(U)$  is of the form  $\{\alpha_i + \rho_c(\lambda_i)\}_{c \in A}$ . It follows that  $\text{Gal}(E(\alpha_i)/E) \subseteq \rho[a_i]$ . Therefore  $\text{Gal}(E(\alpha_i)/E)$  is an elementary  $p$ -abelian group. Since we have the group monomorphism

$$\text{Gal}(L/E) \hookrightarrow \prod \text{Gal}(E(\alpha_i)/E)$$

it follows that  $\text{Gal}(L/E)$  is an elementary  $p$ -abelian group.

**Lemma 6.1.** *Let  $L/E$  be a finite Galois cyclotomic coradical extension. Then*

$$B^1(G, \mu(L)) \cong \mu(L)/\mu(E),$$

where  $G = \text{Gal}(L/E)$ .

*Proof.* The map  $\psi : \mu(L) \rightarrow B^1(G, \mu(L))$  is defined as follows:  $\psi(u) = f_u$ , where  $u \in \mu(L)$  and  $f_u = \sigma(u) - u$  for each  $\sigma \in G$ . It is clear that  $\psi$  is a group isomorphism.  $\square$

Let  $\mu(L) = \rho[a]$  for some  $a \in A$ . We define

$$\deg(\mu(L)) = \deg a.$$

**Proposition 6.2.** *Consider  $A$  with  $h_A = 1$  and let  $L/E$  be a Galois cyclotomic coradical extension. Assume that  $\mu(L) = \mu(E)$  and let  $a \in A$  be such that  $\mu(L) = \rho[a]$ . Then*

$$|\text{Drincog}(L/E)| = q^{m \deg(\mu(L))},$$

where  $m = |G|$  with  $G = \text{Gal}(L/E) \cong C_p^m$ .

*Proof.* First note that  $B^1(G, \mu(L)) = \{0\}$ . On the other hand, since the action of  $G$  is trivial on  $\mu(L)$ , we obtain  $H^1(G, \mu(L)) = \text{Hom}(G, \mu(L))$ . From Theorem 5.3 follows

$$\text{Drincog}(L/E) \cong Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong H^1(G, \mu(L)) = \text{Hom}(G, \mu(L)).$$

Now  $|\mu(L)| = C_p^{s \deg(\mu(L))}$ , so that

$$\begin{aligned} \text{Hom}(G, \mu(L)) &= \text{Hom}(C_p^m, C_p^{s \deg(\mu(L))}) \\ &= \mathfrak{L}_p(\mathbb{F}_p^m, \mathbb{F}_p^{s \deg(\mu(L))}) = \mathfrak{M}_{m \times s \deg(\mu(L))}(\mathbb{F}_p). \end{aligned}$$

Therefore  $|\text{Hom}(G, \mu(L))| = q^{m \deg(\mu(L))}$ .  $\square$

For the following result, we consider  $h_A = 1$  and  $E = K$ .

**Theorem 6.3.** *Let  $L/K$  be a Galois cyclotomic coradical extension and assume that  $L = K(\mu(L))$ . Then  $|\text{Drincog}(L/K)| \leq q^{m \deg(\mu(L))}$ .*

*Proof.* Similar to [7, Proposition 8.5].  $\square$

## 7. CASE $h_A > 1$

The fundamental results we have obtained for the cyclotomic coradical extension with  $A$  having class number one, are not true any longer for  $A$  with  $h_A > 1$ . We give an example showing why the results fail to hold.

Let  $K = \mathbb{F}_q(T)$  with  $p = q = 3$ . Let  $\mathfrak{p}_\infty$  be the place associated to  $T^2 + 1$  and let  $A = \{x \in K \mid v_{\mathfrak{p}}(x) \geq \text{for every place } \mathfrak{p} \neq \mathfrak{p}_\infty\}$ . Then

$$A = \left\{ \frac{G(T)}{(T^2 + 1)^n} \mid G(T) \in \mathbb{F}_q[T], n \in \mathbb{N}, \deg G(T) \leq 2n \right\}.$$

Since  $\mathfrak{p}_\infty$  is of degree 2 and  $h_K = 1$ , we have  $h_A = 2$ .

Let  $\xi = \frac{1}{T^2 + 1}$  and consider  $R_\xi = \mathbb{F}_q[\xi]$ . Let  $\mathbb{F}_q(\xi)$  denote the quotient field of  $R_\xi$ . Then  $A$  is the integral closure of  $R_\xi$  in  $K$ . Using the division algorithm, it follows that if  $x \in A$ , then  $x = \frac{G(T)}{(T^2 + 1)^n}$  with  $\deg G(T) \leq 2n$  and

$$G(T) = \alpha_0 + \alpha_1(T^2 + 1) + \cdots + \alpha_n(T^2 + 1)^n = \alpha_0 + \alpha_1\xi^{-1} + \cdots + \alpha_n\xi^{-n},$$

where  $\alpha_i \in \mathbb{F}_q[T]$  is of degree less than or equal to 1. Furthermore, because  $\deg G(T) \leq n$ , it follows that  $\alpha_n \in \mathbb{F}_q$ .

Therefore

$$\begin{aligned} x &= \frac{G(T)}{(T^2 + 1)^n} = \xi^n G(T) = \alpha_n + \alpha_{n-1}\xi + \cdots + \alpha_1\xi^{n-1} + \alpha_0\xi^n \\ &= \beta_0 + \beta_1\xi + \cdots + \beta_{n-1}\xi^{n-1} + \beta_n\xi^n, \end{aligned}$$

with  $\beta_i = \alpha_{n-1} = a_i + b_iT \in \mathbb{F}_q[T]$ ,  $0 \leq i \leq n$  and  $\beta_0 = a_0$ .

Thus

$$\begin{aligned} (2) \quad x &= \xi^n G(T) = \sum_{i=0}^n a_i \xi^i + T \sum_{i=1}^n b_i \xi^i \\ &= \sum_{i=0}^n a_i \xi^i + (T\xi) \sum_{i=0}^{n-1} b_{i+1} \xi^i = F(\xi) + (T\xi)H(\xi) \end{aligned}$$

with  $F(\xi), G(\xi) \in R_\xi$ ,  $\deg F(\xi) \leq n$ ,  $\deg H(\xi) \leq n - 1$ .

Note that the degree of  $F(\xi)$  in  $T$  is even and the degree of  $(T\xi)H(\xi)$  is odd, so that it follows that  $x = 0 \iff F(\xi) = H(\xi) = 0$ . In particular  $\{1, T\xi\}$  is an integral basis of  $A/R_\xi$ . On the other hand, since  $\xi = \frac{1}{T^2+1}$ , it follows that  $(\xi T)^2 = -\xi^2 + \xi$ . Therefore

$$\ell(Z) := \text{Irr}(Z, T\xi, \mathbb{F}_q(\xi)) = Z^2 + \xi^2 - \xi.$$

Let  $\mathbb{F}_q[X, Y] \xrightarrow{\phi} A$  be given by  $\phi(f(X, Y)) = f(\xi, T\xi)$ . From (2), we obtain that  $\phi$  is a ring epimorphism. Further  $\phi(Y^2 + X^2 - X) = 0$ , that is,  $\langle Y^2 + X^2 - X \rangle \subseteq \ker \phi$  and  $\phi$  induces the epimorphism  $\tilde{\phi}: \mathbb{F}_q[X, Y]/\langle Y^2 + X^2 - X \rangle \rightarrow A$  given by  $\tilde{\phi}(f(X, Y) \bmod \langle Y^2 + X^2 - X \rangle) = f(\xi, T\xi)$ . From (2) follows that  $\tilde{\phi}$  is a ring isomorphism.

We may apply Kummer's Theorem on the decomposition of prime ideals in the ring extension  $A/R_\xi$  since  $A = R_\xi[T\xi]$ . In particular we have

$$\ell(Z) \bmod \xi = Z^2; \quad \ell(Z) \bmod (\xi - 1) = Z^2;$$

so that

$$\begin{aligned} (\xi) &= \mathfrak{p}_\xi^2 \quad \text{with} \quad \mathfrak{p}_\xi = (\xi, T\xi) \quad \text{and} \\ (\xi - 1) &= \mathfrak{p}_{\xi-1}^2 \quad \text{with} \quad \mathfrak{p}_{\xi-1} = (\xi - 1, T\xi), \end{aligned}$$

with  $\mathfrak{p}_\xi$  and  $\mathfrak{p}_{\xi-1}$  prime ideals of  $A$ . Furthermore,  $(T\xi)^2 = \xi(1 - \xi)$ , so that

$$(T\xi) = \mathfrak{p}_\xi \mathfrak{p}_{\xi-1}.$$

Thus,  $\xi, \xi - 1$  and  $T\xi$  are irreducible non prime elements of  $A$  and  $(T\xi)^2 = \xi(1 - \xi)$ .

Let  $\rho: A \rightarrow E\langle\tau\rangle$  be a rank one  $A$ -Drinfeld module, where  $E = K_\rho = H_A$  is the field of definition of  $\rho$ . In fact, since  $\deg \xi = \deg T\xi = 2$ ,  $\rho$  is determined by

$$\rho_\xi = \xi + \gamma_1\tau + \gamma_2\tau^2; \quad \rho_{T\xi} = T\xi + \epsilon_1\tau + \epsilon_2\tau^2$$

and since  $(T\xi)^2 = \xi(1 - \xi)$ , we obtain

$$\rho_{(T\xi)^2} = \rho_{T\xi}\rho_{T\xi} = \rho_\xi(1 - \rho_\xi) = \rho_{\xi(1-\xi)}.$$

Let  $L := E(\lambda_\xi) = E(\rho[\xi])$ . Then  $L/E$  satisfies that  $\text{Gal}(L/E) \cong (A/(\xi))^* = (A/(\mathfrak{p}_\xi)^2)^*$  (Corollary 3.3) and  $\mu_\rho(L) = \rho[\xi]$  (Proposition 3.7). Consider the element

$$\delta := \rho_{T\xi}(\lambda_\xi).$$

Then  $E \subseteq E(\delta) \subseteq L$ . Now,  $G := \text{Gal}(L/E)$  may be identified with  $(A/(\xi))^*$  as follows. Since  $A \cong \mathbb{F}_q[X, Y]/\langle Y^2 + X^2 - X \rangle$ , where  $X$  is identified with  $\xi$  and  $Y$  with  $T\xi$ , and the group identification is done by its action on  $\lambda_\xi$ , then we may write  $G = \{\sigma_U\}_{U \in \{1, 2, 1+y, 2+y, 1+2y, 2+2y\}}$  with  $y = Y \bmod \langle Y^2 + X^2 - X \rangle = T\xi$  and  $\sigma_U(\lambda_\xi) := \rho_U(\lambda_\xi)$ .

We have  $G \cong C_6$  the cyclic group of 6 elements and generated by  $2 + y$ . Further  $(2 + y)^2 = 1 + y$ , that is, the subgroup of  $G$  of order 2 is generated by  $1 + y$ . Note that

$$\sigma_{1+y}(\delta) = \rho_{1+T\xi}(\rho_{T\xi}(\lambda_\xi)) = \rho_{T\xi+(T\xi)^2}(\lambda_\xi) = \rho_{T\xi}(\lambda_\xi) + \rho_{\xi(1-\xi)}(\lambda_\xi) = \delta$$

and

$$\begin{aligned}\sigma_{2+y}(\delta) &= \rho_{2+T\xi}(\rho_{T\xi}(\lambda_\xi)) = \rho_{2T\xi+(T\xi)^2}(\lambda_\xi) \\ &= \rho_{2T\xi}(\lambda_\xi) + \rho_{\xi(1-\xi)}(\lambda_\xi) = 2\delta + 0 \neq \delta,\end{aligned}$$

so that  $E(\delta)$  is the fixed field of the subgroup  $C_3$  of  $G$  and therefore  $[E(\delta) : E] = 2$  and  $[L : E(\delta)] = 3$ .

Note that  $E(\delta)/E$  is a cyclotomic coradical extension and of prime degree  $2 \neq p = q$ . On the other hand, the subextension  $L/E$  is not pure and it is of degree  $3 = p = q$ . All this is contrary to what we established in Proposition 5.5, Corollary 5.6, Lemma 5.8 and to Theorems 5.9, 5.10 and 5.11. In other words, in its actual form, we do not have a cogalois theory for  $A$ -Drinfeld modules of rank one if  $h_A > 1$ .

## 8. THE CARLITZ MODULE

In this section we consider the Carlitz module, more precisely we are interested in computing the cardinality of the module  $\text{Drincog}(L/K)$  where  $L = k(T)(\Lambda_{P^n})$ ,  $K = k(\Lambda_P)$  and  $P \in R_T$  is a monic irreducible polynomial. We also assume that  $\text{char } \mathbb{F}_q = p > 2$ . The goal of this section is to understand why it is so hard to find torsion elements other than the obvious ones  $(\Lambda_{P^n})$ .

We have established the existence of a group isomorphism

$$\phi : \text{Drincog}(L/K) \rightarrow Z^1(G, M)$$

where  $G = \text{Gal}(L/K)$  and  $M = \Lambda_{P^n}$ . Therefore  $\phi(\alpha + K)$  is a crossed homomorphism defined as

$$\phi(\alpha + K)(\sigma) = \sigma(\alpha) - \alpha$$

for each  $\sigma \in G$ . To simplify the notation, frequently we will write  $\phi(\alpha)$  instead of  $\phi(\alpha + K)$ . On the other hand if we have a crossed homomorphism  $f : G \rightarrow M$  it satisfies

$$(3) \quad f(\sigma \cdot \tau) = f(\sigma) + \sigma \cdot f(\tau)$$

for each  $\sigma, \tau \in G$ . We will understand that  $\sigma \cdot f(\tau)$  as the action of  $\sigma$  on  $f(\tau)$ . Since the elements of  $M$  are of the form  $C_D(\lambda_{P^n})$  we may write

$$f(\sigma) = C_{D_\sigma}(\lambda_{P^n}).$$

Further, by the division algorithm, we may assume that  $D_\sigma$  is a polynomial of degree less than or equal to  $\deg P^n = n \deg P$ . Note that with the exponents of the elements  $\sigma$  it is possible to form a system of equations using relation (3) as follows: since  $f(\sigma \cdot \tau) = C_{D_{\sigma \cdot \tau}}(\lambda_{P^n})$  we have

$$(4) \quad C_{D_{\sigma \cdot \tau}}(\lambda_{P^n}) = C_{D_\sigma}(\lambda_{P^n}) + \sigma \cdot C_{D_\tau}(\lambda_{P^n}).$$

Now  $\sigma$  is of the form  $\sigma = 1 + B_\sigma P^s$  with  $\gcd(B_\sigma, P) = 1$  and  $1 \leq s \leq n-1$  (see [5]). Therefore equation (4) can be rewritten as:

$$(5) \quad C_{D_{\sigma \cdot \tau}}(\lambda_{P^n}) = C_{D_\sigma}(\lambda_{P^n}) + \sigma \cdot C_{D_\tau}(\lambda_{P^n}).$$

Since the group  $G$  is commutative and  $\tau = 1 + B_\tau P^t$ , with  $\gcd(B_\tau, P) = 1$  and  $1 \leq t \leq n-1$ , we obtain

$$(6) \quad C_{D_{\sigma \cdot \tau}}(\lambda_{P^n}) = C_{D_\sigma}(\lambda_{P^n}) + C_{(1+B_\tau P^t)D_\sigma} \lambda_{P^n}.$$

Therefore the exponents satisfy the system of equations (modulo  $P^n$ ):

$$(7) \quad D_{\sigma \cdot \tau} = D_\sigma + (1 + B_\sigma P^s)D_\tau,$$

$$(8) \quad D_{\sigma \cdot \tau} = D_\tau + (1 + B_\tau P^t)D_\sigma.$$

If  $\tau = \sigma^{-1}$ , we have

$$(9) \quad 0 = D_\sigma + (1 + B_\sigma P^s)D_\tau.$$

Equation (9) allow us to obtain the possible solutions of system (7) and therefore the number of elements of  $\text{Drincog}(L/K)$ . This can be used as a first rough algorithm to solve the system of equations. First we obtain the multiplication table of the group  $G$ , then we parameterize the possible solutions in a vector with components

$$D_\sigma = -(1 + B_\sigma P^s)D_\tau$$

and finally we verify which of these vectors are really solutions of system (7). One of the most important problems we have with this approach is that, even for very small prime numbers  $p$ , the number of solutions is very large.

This approach allows us to find explicit torsion elements other than the class of  $\lambda_{P^n}$ . We achieve this goal finding the complete list of crossed homomorphisms and then we use the function  $\phi$  to find the values we are interested in, that is, the torsion points of the module  $\text{Drincog}(L/K)$ .

**Example 8.1.** We may apply the previous approach to the following case. Let  $q = p = 3$ ,  $P = T$  and  $n = 2$ . We compute first the multiplication table of  $G$ :

	$\sigma_1$	$\sigma_2$	$\sigma_3$
$\sigma_1$	$\sigma_1$	$\sigma_2$	$\sigma_3$
$\sigma_2$	$\sigma_2$	$\sigma_3$	$\sigma_1$
$\sigma_3$	$\sigma_3$	$\sigma_1$	$\sigma_2$

where  $\sigma_1 = 1$ ,  $\sigma_2 = 1 + T$  and  $\sigma_3 = 1 + 2T$  modulo  $T^2$ , are all the elements of  $G$ . Therefore, in this case, the system equations (7) can be written as follows:

$$(10) \quad D_{\sigma_3} = D_{\sigma_2} + (1 + T)D_{\sigma_2},$$

$$(11) \quad D_{\sigma_2} = -(1 + T)D_{\sigma_3},$$

$$(12) \quad D_{\sigma_2} = D_{\sigma_3} + (1 + 2T)D_{\sigma_3}.$$

Therefore the solutions of the previous system are:

$$(T^2, (2T + 2)D_{\sigma_3}, D_{\sigma_3}),$$

where  $D_{\sigma_3}$  runs through all the polynomials of degree less than or equal to 1, with coefficients in  $\mathbb{F}_q$ . Note that the first component of the previous vector is  $T^2$  since we know that if  $f$  is a crossed homomorphism, we have  $f(1) = 0$ . Therefore the number of solutions of the system (10) is 9. This was already obtained in [7, Example 7.8].

Using the function  $\phi$  it can be shown that  $\phi(\lambda_{T^2}) = f_4$  and  $\phi(C_2(\lambda_{T^2})) = f_7$ . We want to find the rest of the  $\alpha_i$ . To achieve this, note that

$$\alpha_2 = a_0 + a_1 \lambda_{T^2} + a_2 (C_2(\lambda_{T^2}))^2,$$

where  $a_i \in K$  for  $i = 0, 1, 2$ . Now

$$\begin{aligned}\phi(\alpha_2)(\sigma_1) &= 0, \\ \phi(\alpha_2)(\sigma_2) &= a_1(C_{1+T}(\lambda_{T^2}) - \lambda_{T^2}) + a_2((C_{1+T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2), \\ \phi(\alpha_2)(\sigma_3) &= a_1(C_{1+2T}(\lambda_{T^2}) - \lambda_{T^2}) + a_2((C_{1+2T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2).\end{aligned}$$

On the other hand, we want that  $\phi(\alpha_2) = f_2$ . Hence, we obtain the system of equations:

$$\begin{aligned}a_1(C_{1+T}(\lambda_{T^2}) - \lambda_{T^2}) + a_2((C_{1+T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2) &= C_{2T+2}(\lambda_{T^2}), \\ a_1(C_{1+2T}(\lambda_{T^2}) - \lambda_{T^2}) + a_2((C_{1+2T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2) &= \lambda_{T^2}.\end{aligned}$$

The solutions of the system are:

$$\begin{aligned}a_1 &= \frac{\begin{vmatrix} C_{2T+2}(\lambda_{T^2}) & (C_{1+T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2 \\ \lambda_{T^2} & (C_{1+2T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2 \end{vmatrix}}{\begin{vmatrix} C_{1+T}(\lambda_{T^2}) - \lambda_{T^2} & (C_{1+T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2 \\ C_{1+2T}(\lambda_{T^2}) - \lambda_{T^2} & (C_{1+2T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2 \end{vmatrix}}, \\ a_2 &= \frac{\begin{vmatrix} C_{1+T}(\lambda_{T^2}) - \lambda_{T^2} & C_{2T+2}(\lambda_{T^2}) \\ C_{1+2T}(\lambda_{T^2}) - \lambda_{T^2} & \lambda_{T^2} \end{vmatrix}}{\begin{vmatrix} C_{1+T}(\lambda_{T^2}) - \lambda_{T^2} & (C_{1+T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2 \\ C_{1+2T}(\lambda_{T^2}) - \lambda_{T^2} & (C_{1+2T}(\lambda_{T^2}))^2 - (\lambda_{T^2})^2 \end{vmatrix}}.\end{aligned}$$

Proceeding similarly, it is possible to find the rest of the  $\alpha_i$ .

The method of Example 8.1 can be used to other situations, more precisely, to Galois extensions  $L/K$ . In some cases it is possible to describe the lattice of radical extensions.

**Example 8.2.** Let  $q = p = 3$ ,  $P = T$  and  $n = 3$ . The multiplication table of the group  $G$  is:

	$\sigma_1$	$\sigma_2$	$\sigma_3$	$\sigma_4$	$\sigma_5$	$\sigma_6$	$\sigma_7$	$\sigma_8$	$\sigma_9$
$\sigma_1$	$\sigma_1$	$\sigma_2$	$\sigma_3$	$\sigma_4$	$\sigma_5$	$\sigma_6$	$\sigma_7$	$\sigma_8$	$\sigma_9$
$\sigma_2$	$\sigma_2$	$\sigma_3$	$\sigma_1$	$\sigma_5$	$\sigma_9$	$\sigma_7$	$\sigma_8$	$\sigma_6$	$\sigma_4$
$\sigma_3$	$\sigma_3$	$\sigma_1$	$\sigma_2$	$\sigma_9$	$\sigma_4$	$\sigma_8$	$\sigma_6$	$\sigma_7$	$\sigma_5$
$\sigma_4$	$\sigma_4$	$\sigma_5$	$\sigma_9$	$\sigma_7$	$\sigma_8$	$\sigma_3$	$\sigma_1$	$\sigma_2$	$\sigma_6$
$\sigma_5$	$\sigma_5$	$\sigma_9$	$\sigma_4$	$\sigma_8$	$\sigma_6$	$\sigma_1$	$\sigma_2$	$\sigma_3$	$\sigma_7$
$\sigma_6$	$\sigma_6$	$\sigma_7$	$\sigma_8$	$\sigma_3$	$\sigma_1$	$\sigma_5$	$\sigma_9$	$\sigma_4$	$\sigma_2$
$\sigma_7$	$\sigma_7$	$\sigma_8$	$\sigma_6$	$\sigma_1$	$\sigma_2$	$\sigma_9$	$\sigma_4$	$\sigma_5$	$\sigma_3$
$\sigma_8$	$\sigma_8$	$\sigma_6$	$\sigma_7$	$\sigma_2$	$\sigma_3$	$\sigma_4$	$\sigma_5$	$\sigma_9$	$\sigma_1$
$\sigma_9$	$\sigma_9$	$\sigma_4$	$\sigma_5$	$\sigma_6$	$\sigma_7$	$\sigma_2$	$\sigma_3$	$\sigma_1$	$\sigma_8$

where  $\sigma_1 = 1$ ,  $\sigma_2 = 2T^2 + T + 1$ ,  $\sigma_3 = 2T^2 + 2T + 1$ ,  $\sigma_4 = T^2 + T + 1$ ,  $\sigma_5 = T^2 + 2T + 1$ ,  $\sigma_6 = T + 1$ ,  $\sigma_7 = 2T + 1$ ,  $\sigma_8 = T^2 + 1$  and  $\sigma_9 = 2T^2 + 1$ .

Using Matlab all the solutions were obtained and

$$|\text{Drincog}(L/K)| = 27 = 3^3.$$

A refinement of [7, Proposition 7.2] allows us to find all the subextensions  $L'/K$  of  $L/K$  that are simple radical, namely:

$$K_1 = L^{\{\sigma_1, \sigma_8, \sigma_9\}}, K_2 = L^{\{\sigma_1, \sigma_5, \sigma_6\}}, K_3 = L^{\{\sigma_1, \sigma_2, \sigma_3\}}, \text{ and } K_4 = L^{\{\sigma_1, \sigma_4, \sigma_7\}}.$$

## REFERENCES

- [1] L. DENIS, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann. **294** (1992), 213–223.
- [2] D. GHIOCA AND L-C HSIA, *Torsion points in families of Drinfeld modules*, Acta Arith. **161** (2013), no. 3, 219–240.
- [3] C. GREITHER AND D.K. HARRISON, *A Galois correspondence for radical extensions of fields*, Pure Appl. Algebra **43** (1986), 257–270.
- [4] D. HAYES, *A brief introduction to Drinfeld modules*, The arithmetic of function fields (Columbus, OH, 1991), 1–32, Ohio State Univ. Math. Res. Inst. Publ., **2**, de Gruyter, Berlin, 1992.
- [5] P. LAM-ESTRADA AND G. VILLA-SALVADOR, *Some remarks on the theory of cyclotomic function fields*, Rocky Mountain Journal of Mathematics **31** (2001), no. 2, 483–502.
- [6] B. POONEN, *Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture*, Math. Ann. **308** (1997), no. 4, 571–586.
- [7] M. SÁNCHEZ-MIRAFUENTES AND G. VILLA-SALVADOR, *Radical extensions for the Carlitz module*, Journal of Algebra, **398** (2014), 284–302.
- [8] F. SCHULTHEIS, *Carlitz-Kummer Function Fields*, Journal of number theory **36** (1990), 133–144.
- [9] A. SCHWEIZER, *On the uniform boundedness conjecture for Drinfeld modules*, Math. Z. **244** (2003), 601–614.
- [10] G. VILLA-SALVADOR, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.

*E-mail address:* kmasml1969@yahoo.com.mx

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.

*E-mail address:* jcostorres88@hotmail.com, torresljcesar0@gmail.com

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.

*E-mail address:* gvillasalvador@gmail.com, gvilla@ctrl.cinvestav.mx